In the Claims

1. (Currently amended) A security system for a computer system, comprising:

a plurality of assets within the computer system;

a plurality of members registered to use the computer system;

a plurality of roles defining user rights to access one or more of the plurality of assets, each member ~~having~~ associated with at least one role;

a plurality of access control lists each corresponding to ~~the assets, each list~~ an asset and defining at least one privilege for accessing the asset corresponding to the privilege, according to a member's role; and

at least one domain being an administrative and access control boundary around a plurality of security entities, ~~each domain having~~ the security entities of the at least one domain comprising:

a subset of the plurality of assets and ~~corresponding~~ the access control lists corresponding to the assets in the subset of the assets;~~, and~~

a subset of the plurality of roles; and

a subset of the members;

each privilege defined in the access control lists of the at least one domain identifying one or more roles in the domain that may access the asset corresponding to the privilege;

~~wherein access is allowed by~~ the security system operable to authorize a particular member to perform a requested operation with respect to a requested asset within ~~a domain~~ the domain when ~~that~~ the particular member ~~has~~ is associated with a role, in the domain, corresponding to a privilege for ~~that~~ the requested asset.

2. (Currently amended) The system of Claim 1, wherein:

the privileges for each asset include ~~actions~~ operations that can be performed on that asset~~, and wherein~~; and

the security system is operable to authorize access ~~is allowed~~ the requested asset when a requested access ~~by a~~ by the particular member includes an ~~action~~ operation to be performed ~~form~~ from the access control list and the particular member is associated with a role, in the domain, corresponding to a privilege for the requested asset.

3. (Currently amended) The system of Claim 1, wherein the ~~privileges include~~ at least one privilege includes one or more of:

a read privilege;

a modify privilege; and

a delete privilege.

4. (Canceled)

5. (Canceled)

6. (Original) The system of Claim 1, wherein the system includes at least two domains.

7. (Currently amended) A method for providing secure access to a plurality of assets within a computer system, comprising ~~the steps of~~:

registering a plurality of members to use the computer system;

providing a plurality of roles defining user rights to access one or more of the plurality of assets, each member associated with at least one role;

providing a plurality of access control lists each corresponding to an asset and defining at least one privilege for accessing the asset corresponding to the privilege, according to a member's role;

providing at least one domain defining an administrative and access control boundary around a plurality of security entities, the security entities of the at least one domain comprising:

a subset of the plurality of assets and the access control lists corresponding to the assets in the subset of the assets;

a subset of the plurality of roles; and

a subset of the members;

each privilege defined in the access control lists of the at least one domain identifying one or more roles in the domain that may access the asset corresponding to the privilege;

when a ~~user~~ particular member attempts to access ~~an~~ a requested asset within ~~a domain~~ the at least one domain, determining ~~a at~~ at least one role assigned to the ~~user~~ particular member;

comparing rights corresponding to the role assigned to the ~~user~~ particular member to ~~a list of privileges~~ the privileges defined in the access control list corresponding to the particular asset; and

if the attempted access is ~~allowed for a~~ authorized for the role assigned to the ~~user~~ particular member, allowing the ~~user~~ particular member to access the requested asset.

8. (Original) The method of Claim 7, wherein a requested access is one from the types read, modify, or delete.

9. (Currently amended) The method of Claim 7, further ~~comprising the step of:~~ comprising, prior to the ~~user~~ particular member attempting to access ~~any assets,~~ the requested asset:

authenticating the ~~user's~~ particular member's identification~~, and~~; and

assigning at least one role to the ~~user~~ particular member.

10. (New) The system of Claim 6, wherein the plurality of roles comprise one or more of:

a domain role defining user rights within a single domain; and

a universal role defining user rights across a plurality of domains.

11. (New) The system of Claim 6, wherein a first domain and a second domain are joined by a unidirectional trust relationship, allowing privileges associated with the first domain's assets to be delegated to the second domain.

12. (New) The system of Claim 6, wherein a first domain and a second domain are joined by a bidirectional trust relationship, allowing:

privileges associated with the first domain's assets to be delegated to the second domain; and

privileges associated with the second domain's assets to be delegated to the first domain.

13. (New) The system of Claim 6, wherein a first domain owns a second domain such that the first domain can create and destroy the second domain.

14. (New) The system of Claim 1, wherein the plurality of roles are assigned to a plurality of user groups, each user group comprising one or more of the plurality of members.

15. (New) The system of Claim 1, wherein each of the plurality of access control lists comprises a plurality of access control entries, each comprising:

a domain identifier;

a role identifier; and

one or more privileges.

16. (New) The system of Claim 1, wherein:

the system comprises at least two domains; and

the system is further operable to grant the particular member, which is assigned a particular domain/role combination, ownership of a particular operation on a particular access control list, ownership over of the particular access control list allowing the particular member to grant rights to perform the operation to one or more members in a different domain than the particular member that are assigned the same role as the particular member.

17. (New) The system of Claim 1, wherein:

one or more of the plurality of assets each comprise a registered asset, a registered asset being a resource that is protected by the security system; and

each registered asset is classified according to a corresponding asset type, which determines how its corresponding registered assets are identified and what operations may be performed on its corresponding registered assets.

18. (New) The system of Claim 1, wherein the security system is operable to authorize access to the requested asset by:

receiving from the particular member a request to access the requested asset, the request comprising:

an identification of the requested asset;

an identification of an operation to perform with respect to the requested asset; and

an identification of the domain and role assigned to the particular member;

determining, based at least in part on the access control list corresponding to the requested asset and the domain and role assigned to the particular member, whether the particular member may perform the identified operation with respect to the requested asset; and

initiating an appropriate action based on the authorization determination.

19. (New) The system of Claim 1, wherein the security system is operable to:

receive from the particular member a request comprising:

one or more query criteria specifying one or more assets; and

an identification of the domain and role assigned to the particular member;

add appropriate security-related criteria to the request;

execute a query to determine one or more assets satisfying the query criteria to which the particular member has read access; and

initiate an appropriate action based on results of the executed query.

20. (New) The system of Claim 1, further operable to:

receive a request to define a new asset type, the request comprising one or more of a name of the new asset type, a description of the new asset type; and a format of the new asset type;

enable determination of one or more operations that should apply to the new asset type; and

enable association of the determined one or more operations with the new asset type.

21. (New) The system of Claim 1, further operable to, prior to the particular member attempting to access the requested asset:

authenticate the particular member's identification; and

assign at least one role to the particular member.

22. (New) The method of Claim 7, further comprising providing at least two domains.

23. (New) The method of Claim 22, wherein the plurality of roles comprise one or more of:

a domain role defining user rights within a single domain; and

a universal role defining user rights across a plurality of domains.

24. (New) The method of Claim 22, wherein a first domain and a second domain are joined by a unidirectional trust relationship, allowing privileges associated with the first domain's assets to be delegated to the second domain.

25. (New) The method of Claim 22, wherein a first domain and a second domain are joined by a bidirectional trust relationship, allowing:

privileges associated with the first domain's assets to be delegated to the second domain; and

privileges associated with the second domain's assets to be delegated to the first domain.

26. (New) The method of Claim 22, wherein a first domain owns a second domain such that the first domain can create and destroy the second domain.

27. (New) The method of Claim 7, wherein the plurality of roles are assigned to a plurality of user groups, each user group comprising one or more of the plurality of members.

28. (New) The method of Claim 7, wherein each of the plurality of access control lists comprises a plurality of access control entries, each comprising:

a domain identifier;

a role identifier; and

one or more privileges.

29. (New) The method of Claim 7, further comprising:

providing at least two domains; and

granting the particular member, which is assigned a particular domain/role combination, ownership of a particular operation on a particular access control list, ownership over of the particular access control list allowing the particular member to grant rights to perform the operation to one or more members in a different domain than the particular member that are assigned the same role as the particular member.

30. (New) The method of Claim 7, wherein:

one or more of the plurality of assets each comprise a registered asset, a registered asset being a resource for which secure access is provided; and

each registered asset is classified according to a corresponding asset type, which determines how its corresponding registered assets are identified and what operations may be performed on its corresponding registered assets.

31. (New) The method of Claim 7, further comprising authorizing access to the requested asset by:

receiving from the particular member a request to access the requested asset, the request comprising:

an identification of the requested asset;

an identification of an operation to perform with respect to the requested asset; and

an identification of the domain and role assigned to the particular member;

determining, based at least in part on the access control list corresponding to the requested asset and the domain and role assigned to the particular member, whether the particular member may perform the identified operation with respect to the requested asset; and

initiating an appropriate action based on the authorization determination.

32. (New) The method of Claim 7, further comprising:

receiving from the particular member a request comprising:

one or more query criteria specifying one or more assets; and

an identification of the domain and role assigned to the particular member;

adding appropriate security-related criteria to the request;

executing a query to determine one or more assets satisfying the query criteria to which the particular member has read access; and

initiating an appropriate action based on results of the executed query.

33. (New) The method of Claim 7, further comprising:

receiving a request to define a new asset type, the request comprising one or more of a name of the new asset type, a description of the new asset type; and a format of the new asset type;

enabling determination of one or more operations that should apply to the new asset type; and

enabling association of the determined one or more operations with the new asset type.

34. (New) Software for providing secure access to a plurality of assets within a computer system, the software embodied in computer-readable media and when executed using one or more computer systems operable to:

register a plurality of members to use the computer system;

provide a plurality of roles defining user rights to access one or more of the plurality of assets, each member associated with at least one role;

provide a plurality of access control lists each corresponding to an asset and defining at least one privilege for accessing the asset corresponding to the privilege, according to a member's role;

provide at least one domain defining an administrative and access control boundary around a plurality of security entities, the security entities of the at least one domain comprising:

a subset of the plurality of assets and the access control lists corresponding to the assets in the subset of the assets;

a subset of the plurality of roles; and

a subset of the members;

each privilege defined in the access control lists of the at least one domain identifying one or more roles in the domain that may access the asset corresponding to the privilege;

when a particular member attempts to access a requested asset within the at least one domain, determine at least one role assigned to the particular member;

compare rights corresponding to the role assigned to the particular member to the privileges defined in the access control list corresponding to the particular asset; and

if the attempted access is authorized for the role assigned to the particular member, allow the particular member to access the requested asset.

34. (New) The software of Claim 34, wherein a requested access is one from the types read, modify, or delete.

35. (New) The software of Claim 34, further operable to, prior to the particular member attempting to access the requested asset:

authenticate the particular member's identification; and

assign at least one role to the particular member.

36. (New) The software of Claim 34, operable to provide at least two domains.

37. (New) The software of Claim 36, wherein the plurality of roles comprise one or more of:

a domain role defining user rights within a single domain; and

a universal role defining user rights across a plurality of domains.

38. (New) The software of Claim 36, wherein a first domain and a second domain are joined by a unidirectional trust relationship, allowing privileges associated with the first domain's assets to be delegated to the second domain.

39. (New) The software of Claim 36, wherein a first domain and a second domain are joined by a bidirectional trust relationship, allowing:

privileges associated with the first domain's assets to be delegated to the second domain; and

privileges associated with the second domain's assets to be delegated to the first domain.

40. (New) The software of Claim 36, wherein a first domain owns a second domain such that the first domain can create and destroy the second domain.

41. (New) The software of Claim 34, wherein the plurality of roles are assigned to a plurality of user groups, each user group comprising one or more of the plurality of members.

42. (New) The software of Claim 34, wherein each of the plurality of access control lists comprises a plurality of access control entries, each comprising:

a domain identifier;

a role identifier; and

one or more privileges.

43. (New) The software of Claim 34, further operable to:

provide at least two domains; and

grant the particular member, which is assigned a particular domain/role combination, ownership of a particular operation on a particular access control list, ownership over of the particular access control list allowing the particular member to grant rights to perform the operation to one or more members in a different domain than the particular member that are assigned the same role as the particular member.

44. (New) The software of Claim 34, wherein:

one or more of the plurality of assets each comprise a registered asset, a registered asset being a resource for which secure access is provided; and

each registered asset is classified according to a corresponding asset type, which determines how its corresponding registered assets are identified and what operations may be performed on its corresponding registered assets.

45. (New) The software of Claim 34, further operable to authorize access to the requested asset by:

receiving from the particular member a request to access the requested asset, the request comprising:

an identification of the requested asset;

an identification of an operation to perform with respect to the requested asset; and

an identification of the domain and role assigned to the particular member;

determining, based at least in part on the access control list corresponding to the requested asset and the domain and role assigned to the particular member, whether the particular member may perform the identified operation with respect to the requested asset; and

initiating an appropriate action based on the authorization determination.

46. (New) The software of Claim 34, further operable to:

receive from the particular member a request comprising:

one or more query criteria specifying one or more assets; and

an identification of the domain and role assigned to the particular member;

add appropriate security-related criteria to the request;

execute a query to determine one or more assets satisfying the query criteria to which the particular member has read access; and

initiate an appropriate action based on results of the executed query.

47. (New) The software of Claim 34, further operable to:

receive a request to define a new asset type, the request comprising one or more of a name of the new asset type, a description of the new asset type; and a format of the new asset type;

enable determination of one or more operations that should apply to the new asset type; and

enable association of the determined one or more operations with the new asset type.